Project 1: Automated ELK Stack Deployment
Question 1: Cloud Access Control

How would you control access to a cloud network?

1. Restate the Problem
I controlled access to a cloud network by creating a public web server in an Azure environment called “RedTeamNet” and a private “ELK-Net” cloud environment for an ELK stack. The RedTeamNet environment provides a web server with two server redundancies (Web 2 & Web 3), and a Jumpbox and Ansible container intended to be an input on system health and log metrics for the ELK stack. The ELK-Net environment is where the live infrastructure for Elastic, Logstash, & Kibana exists.

2. Provide a Concrete Example Scenario
- In Project 1, did you deploy an on-premises or cloud network?
  I deployed a cloud network in Project 1, using Windows Azure as a platform for a two-pronged cloud infrastructure system, creating redundancies and the back end support for the ELK stack and gathering of log data in metrics.
- Did you have to configure access controls to this network?
  Yes.
- What kinds of access controls did you configure, and why were they necessary?
  A Jumpbox was configured because any potential attacker would need to connect to the Jumpbox to access the backend of the system, which is difficult due the heightened security controls in place to access the ELK stack. This silo approach narrows the number of potential pathways an attacker could use to access a system.
- How do these details relate to the interview question?
  Putting strict access controls in place like a Jumpbox and inbound/outbound rules, ultimately create a more secure cloud network environment, and the ELK stack allows us to monitor the health of the system.

3. Explain the Solution Requirements
In Project 1, what kinds of access controls did you have to implement? Consider:
- NSGs around the VNet? Around the VMs?
  The network security groups (NSG’s) I configured include “ELKAccessPort”, an NSG I used to only allow secure access via Port 5601 to our ELK Stack, and creating clear separation between my public Web VMs on RedTeamNet. An NSG focused on SSH access only in Port 22 creates additional access controls.
- Local firewalls (ufw, etc.) on each VM?
  Only one firewall was created as a buffer between the client machine and the load balancer.
- Protocol allow/deny lists?
  Additional protocols were put in place inside our NSGs, including restricting all inbound traffic, and only allowing traffic in from the Azure load balancer & virtual network, including Docker/Ansible containers.

- What did each access control achieve, and why was this restriction necessary for the project?
  Creating restrictions on which port is required for entry, the use of a jumpbox, and redundancies in our web machines, ultimately creates a more resilient & tamperproof network.

4. Explain the Solution Details
   - Which rules do you set for each NSG in the network?
     In the two NSG's ("RedTeamSecurityGroup" and "ELK-server-nsg"), there are three rules, including SSH access in and out of the jumpbox, and access permissions requiring use of Port 80.
   - How does access to the jump box work?
     Traffic from the client computer enters the Azure environment through the firewall, then connects through a load balancer & the three Web machines to get to the jumpbox.
   - How does access from the jump box to the web servers work?
     Web-1 is the primary Web machine that can access the jumpbox, and Web-2 / Web-3 are considered redundancies if Web-1 goes down after passing through the load balancer.

5. Identify Advantages/Disadvantages of the Solution
   - Does your solution scale?
     While the Jumpbox is convenient for this project, it is not very scalable to larger networks that may contain hundreds of machines. Using this solution is a much larger network environment could cause a bottleneck and strain cloud system resources, ultimately creating a single point of failure.
   - Is there a better solution than a jump box?
     Due to long standing vulnerabilities with the jumpbox, ultimately, a domainless solution for architecture, which treats all network traffic as suspicious, allows administrators to create secure channels for very narrow applications on a role by role basis for employers. This forces each piece of IT infrastructure to be independently authenticated, spreading out the potential vulnerabilities, and ultimately makes getting access harder. This gets around some of the issues with a Jumpbox being a high value target, and being a single point of failure.
   - What are the disadvantages of implementing a VPN that kept you from doing it this time?
     Due to not being in control of the security settings from a given client device, if a client computer was compromised, it might give an authorized pipeline to an otherwise unauthorized party to a corporate network. Further, a VPN is visible on the public internet, and potential cybercriminals could scout out the VPN to determine potential vulnerabilities.
   - What are the advantages of a VPN?
     A VPN will mask the private information of a device in use, indicating it is in a different location than its actual physical location. It also removes the proximity requirement of needing to be near a particular network.

- When is it appropriate to use a VPN?
  It is appropriate to use a VPN when you want employees or contractors who are far away from the physical location of the server location to connect to the network.